

1 **DIGITAL SIGNATURE VERIFICATION AND PROGRAM TRANSMISSION**

2 **FIELD OF THE INVENTION**

3 The present invention relates to providing a digital
4 signature for a message exchanged through business message
5 communication via the Internet, and for verifying the
6 signature, so as to authorize the message and a transaction.

7 **BACKGROUND OF THE INVENTION**

8 As the techniques used for a network, such as the Internet,
9 have been developed, a business form by which trading and
10 operations are performed through messages communicated via a
11 network has become popular. For this form, the provision of
12 security is very important.

13 An XML digital signature technique has gradually been
14 established as a data exchange format for use for business
15 communications transmitted across a network, and it is
16 anticipated that the authentication of negotiable
17 instruments and secured transactions can also be effected by
18 applying the XML digital signature technique. A digital
19 signature technique is a technique by which signature
20 information (as digital information) is added to and used
21 for authenticating a digital document. Generally, to

1 provide a signature in such a case, public key cryptography
2 is used. In this case, a signatory prepares signed text by
3 using hashing to prepare a hash of a compressed document and
4 a secret key that only the signer knows, and transmits the
5 original document with the hash. A verifier (a recipient)
6 employs the public key of the signatory and the original
7 document to determine whether the signature is authentic.

8 The digital signature technique also includes a function for
9 preventing a third party or a recipient (a verifier) from
10 counterfeiting or forging a signature, and a function for
11 preventing a signatory from disavowing his or her signature.

12 Thus, when a variety of messages are signed using a unique
13 ID number, a function can be implemented for proving that:

- 14 1. a message was prepared by a sender,
- 15 2. a message was not altered,
- 16 3. the same message was not erroneously received twice,
17 and/or
- 18 4. a message was transmitted by a sender.

19 However, to sign and verify a message using a conventional
20 cryptography library, an application program that employs
21 the digital signature technique must be changed, and this
22 can be quite expensive.

23 In some cases, a digital signature condition may be
24 established to increase the probative force of a digital
25 signature. As an example, for one digital signature
26 technique, a time limit may be set according to which a

1 signature can be provided only within a predetermined time
2 period, or for another digital signature technique, a
3 condition may be established according to which a signature
4 can not be provided unless a specific process is performed.
5 In these cases, when a specific digital signature is
6 provided as a replacement for an original digital signature,
7 and later, the original digital signature is provided as a
8 post signature, it is convenient for the performance of the
9 operation procedures.

10 At the same time as a digital signature is provided and
11 verified, the signed message must be stored in a safe log in
12 order to enable the following monitoring. While the stored
13 message can not be altered because it is accompanied by the
14 signature, the message can be browsed. However, since
15 confidential information may be included in a business
16 message, access control is required for a log.

17 SUMMARY OF THE INVENTION

18 It is, therefore, one aspect of the invention to mount a
19 proxy server that constitutes means for providing, verifying
20 and logging a digital signature for a message that is to be
21 exchanged via a network, so that a security function for a
22 digital signature can be implemented without the application
23 program being changed.

24 It is another aspect of the invention to provide a post

1 signing method by using a proxy server to control a digital
2 signature and its verification.

3 It is an additional aspect of the invention to enable access
4 control for the log of a message by using a proxy server to
5 log a message.

6 To achieve the above aspects, according to the invention, a
7 proxy server for relaying communications between
8 applications and for performing an additional process
9 comprises: a key manager for managing multiple keys used to
10 generate a digital signature to be provided for a message
11 document that is exchanged between the applications; a
12 signature key determiner for extracting the message document
13 from a predetermined application, and for determining a key
14 used to provide a digital signature based on the message
15 document; and a signature generator for providing a digital
16 signature for the message document by using the key that is
17 obtained from the key manager based on a determination made
18 by the signature key determiner, and for transmitting the
19 message document with the digital signature to a destination
20 application. With this arrangement, digital signatures
21 having different security levels can be provided in
22 accordance with the contents of a message document.

23 In addition to the above arrangement, the proxy server of
24 the invention further comprises: a log manager for storing
25 the message document with a digital signature provided by
26 the signature generator, and for managing a log.

1 Also included is a digital signature system is provided
2 using the above described proxy server. The digital
3 signature system comprises: applications for performing data
4 processing; and a proxy server connected to the applications
5 via a network, wherein the proxy server intercepts a
6 communication, transmitted through the network, from an
7 application to an external destination device, provides a
8 digital signature for a message document exchanged via the
9 communication, and transmits the message document with the
10 digital signature to the external destination device.

11 In addition, the present invention provides a digital
12 signature verification system having the following
13 configuration is provided. The digital signature
14 verification system comprises: applications for performing
15 data processing; and a proxy server connected to the
16 applications via a network, wherein the proxy server
17 intercepts a communication from an external destination
18 device to an application transmitted through the network,
19 verifies a digital signature provided for a message document
20 exchanged via the communication, and transmits the message
21 document that has been authorized.

22 Also provided is a digital signature method for providing a
23 digital signature for a message document exchanged by
24 applications and for authorizing the message document
25 comprises the steps of: selecting, in accordance with the
26 type of a message document transmitted by a predetermined
27 application, a key used for providing a digital signature
28 for the message document; providing a digital signature for

1 the message document, when key selection rules set for the
2 key are not established, by using a replacement key that is
3 set in advance for the key; transmitting the message
4 document with the digital signature to a destination
5 designated by the application; and using the key, when the
6 key selection rules for the key have been satisfied after
7 the digital signature has been provided using the
8 replacement key, to again provide a digital signature, and
9 transmitting the message document with the digital signature
10 to the destination.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects, features, and advantages of the present invention will become apparent upon further consideration of the following detailed description of the invention when read in conjunction with the drawing figures, in which:

- Fig. 1 is a diagram for explaining the general configuration of a digital signature system according to one example embodiment of the present invention;
- Fig. 2 is a diagram showing an example configuration of a signature server for adding a digital signature according to the embodiment, of Fig. 1;
- Fig. 3 is a diagram showing an example configuration of a

1 signature server for verifying a digital signature according
2 to the embodiment;

3 Fig. 4 is an example of a flowchart for explaining the
4 signing processing; including a case wherein the original
5 secret key is not available.

6 Fig. 5 is a flowchart for explaining the signing processing
7 performed when the original secret key is available because
8 the acquisition condition has been satisfied; and

9 Fig. 6 is a diagram showing an example key selection rule
10 written in the XML form.

DESCRIPTION OF THE SYMBOLS

- 10: Application
- 20: Signature server
- 21: Signature key determiner
- 22: Key manager
- 23: Signature key acquisition unit
- 24: Signature generator
- 25: Log manager
- 30: Switch
- 40: Firewall
- 100: LAN
- 200: Network

1 DESCRIPTION OF THE INVENTION

2 The present invention provides a proxy server for relaying
3 communications between applications and for performing an
4 additional process comprises: a key manager for managing
5 multiple keys used to generate a digital signature to be
6 provided for a message document that is exchanged between
7 the applications; a signature key determiner for extracting
8 the message document from a predetermined application, and
9 for, based on the message document, determining a key used
10 to provide a digital signature; and a signature generator
11 for providing a digital signature for the message document
12 by using the key that is obtained from the key manager based
13 on a determination made by the signature key determiner, and
14 for transmitting the message document with the digital
15 signature to a destination application. With this
16 arrangement, digital signatures having different security
17 levels can be provided in accordance with the contents of a
18 message document.

19 The key manager sets multiple key selection rules for
20 obtaining the key, and only when the key selection rules are
21 satisfied can the signature generator obtain the key.
22 That is, since a specific condition is to be satisfied to
23 obtain the key, the reliability of the digital signature
24 using the key can be improved. The acquisition condition
25 can be a time condition for limiting the time period within
26 which the key can be used, or a processing condition for
27 inhibiting the use of the key after a specific process has

1 been performed for the message document.

2 When the key for generating a digital signature for the
3 message document can not be obtained because the acquisition
4 condition established for the key has not been satisfied the
5 signature generator can employ a replacement key that is
6 defined in advance to provide a digital signature.

7 In this case, after the signature generator has provided a
8 digital signature using the replacement key, when the
9 acquisition condition that is determined for the original
10 key based on the message document is satisfied to enable the
11 acquisition of the original key, the signature generator can
12 again provide a digital signature using the original key.
13 The post signing may be additionally performed for the
14 signed message document, or may be newly performed for the
15 message document before it is signed using the replacement
16 key.

17 In addition to the above arrangement, the proxy server of
18 the invention further comprises: a log manager for storing
19 the message document with a digital signature provided by
20 the signature generator, and for managing a log.

21 As is described above, to newly perform the post signing for
22 the message document before it is signed using a replacement
23 key, the log manager stores not only the message document
24 for which the signature generator has provided a digital
25 signature using the replacement key, but also the message
26 document without the digital signature. The signature
27 generator obtains, from the log manager, the message
28 document without the digital signature, and provides a

1 digital signature using the original key.
2 Further, according to the invention, a digital signature
3 system having the following configuration is provided using
4 the above described proxy server. The digital signature
5 system comprises: applications for performing data
6 processing; and a proxy server connected to the applications
7 via a network, wherein the proxy server intercepts a
8 communication, transmitted through the network, from an
9 application to an external destination device, provides a
10 digital signature for a message document exchanged via the
11 communication, and transmits the message document with the
12 digital signature to the external destination device.

13 In the digital signature system, the proxy server is
14 connected to the network by a hardware or software switch
15 that enables the interception of information transmitted
16 across the network without the sender and the recipient
17 being aware of it. This switch can be a layer 4 switch.
18 Since a communication transmitted by an application can be
19 intercepted, the digital signature can be provided for the
20 message document without the application being changed,
21 i.e., without the application being aware of the digital
22 signature.

23 Furthermore, according to the invention, a digital signature
24 verification system having the following configuration is
25 provided. The digital signature verification system
26 comprises: applications for performing data processing; and
27 a proxy server connected to the applications via a network,

1 wherein the proxy server intercepts a communication from an
2 external destination device to an application transmitted
3 through the network, verifies a digital signature provided
4 for a message document exchanged via the communication, and
5 transmits the message document that has been authorized.

6 In the digital signature verification system, the proxy
7 server can be connected to the network via a switch, such as
8 a layer 4 switch. Since a communication with an external
9 device via the network can be intercepted, the digital
10 signature of a message document can be verified without the
11 application being changed, i.e., without the application
12 being aware of the digital signature.

13 In addition, according to the invention, a network system
14 comprises: multiple groups connected to a wide area network,
15 all of which have applications for performing data
16 processing and proxy servers connected to the applications
17 via a local area network, wherein the proxy server
18 intercepts a communication transmitted by an application of
19 a local group to an application of a different group,
20 provides a digital signature for a message document
21 exchanged via the communication, and transmits the message
22 document with the digital signature to the application of
23 the different group, and wherein the proxy server intercepts
24 a communication from the application of the different group
25 to the application of the local group, verifies a digital
26 signature provided for a message document exchanged via the
27 communication, and transmits the authorized message document
28 to the application of the local group.

1 When the application of the local group transmits a message
2 document, the proxy server stores the message document with
3 a digital signature in a log, and manages the log. When the
4 application of the local group receives a message document
5 from a different group, the proxy server stores in a log a
6 message document authenticated by a verification of a
7 digital signature, and manages the log. At a predetermined
8 timing, the proxy server compares the transmission log with
9 the reception log for the same message document, and
10 authorizes communication.

11 The information to be compared need not be all the
12 information in the logs; signature information for a digital
13 signature concerning the same message document, or a hash
14 value used for providing a digital signature for the same
15 message document can be compared. In this case, when the
16 information in the logs is the same, the communication can
17 be authorized. When the information differs, a detailed
18 verification is conducted and all the information in the
19 logs is compared.

20 According to the invention, an example of a digital
21 signature method for providing a digital signature for a
22 message document exchanged by applications and for
23 authorizing the message document comprises the steps of:
24 selecting, in accordance with the type of a message document
25 transmitted by a predetermined application, a key used for
26 providing a digital signature for the message document;
27 providing a digital signature for the message document, when
28 key selection rules set for the key are not established, by

1 using a replacement key that is set in advance for the key;
2 transmitting the message document with the digital signature
3 to a destination designated by the application; and using
4 the key, when the key selection rules for the key have been
5 satisfied after the digital signature has been provided
6 using the replacement key, to again provide a digital
7 signature, and transmitting the message document with the
8 digital signature to the destination.

9 According to the invention, a digital signature verification
10 method for verifying a digital signature provided for a
11 message document exchanged by applications, and for
12 authorizing the message document comprises the steps of:
13 accepting a message document with a digital signature that
14 uses a replacement key, when the digital signature on the
15 received message document has been provided by using the
16 replacement key for an original key that is determined in
17 accordance with the type of the message document; receiving
18 a message document, after the message document signed using
19 the replacement key has been accepted, with a digital
20 signature that used the original key; and verifying a
21 digital signature, provided using the original key, to
22 authorize the message document with the digital signature
23 that uses the replacement key.

24 Further, the present invention is applicable as a program
25 that permits a computer to perform the processes
26 corresponding to the steps of the digital signature method
27 and the digital signature verification method, or as a
28 program product that controls a computer that carries out

1 the functions of a proxy server, and a storage medium on
2 which this program is stored and a transmission apparatus
3 for transmitting the program can be provided.

4 **AN ADVANTAGEOUS EMBODIMENT**

5 An example of an advantageous embodiment of the present
6 invention will now be described in detail while referring to
7 the accompanying drawings. Figure 1 is a diagram for
8 explaining the general configuration of a digital signature
9 system according to the embodiment. In Figure 1, company A
10 and company B each include: applications 10 for performing
11 message communication; and a signature server 20 for
12 managing a digital signature provided for messages exchanged
13 by the applications 10. The applications 10 are computers
14 that are controlled by predetermined programs and that
15 implement various functions, including the communication.
16 In Figure 1, the applications 10 and the signature servers
17 20 are separately provided based on their functions, and the
18 arrangement shown does not always apply to the hardware
19 configuration. That is, the applications 10 and the
20 signature server 20 may be formed as separate hardware
21 units, or several applications 10 may be operated using the
22 same hardware.

23 As is shown in Figure 1, the companies A and B are connected
24 via a wide area network 200, such as an Internet, and the
25 application 10 in each company is connected to a LAN 100,
26 such as an in-house network, and to the network 200 via a

1 firewall 40. The signature server 20 in each company is
2 connected to the LAN 100 via a switch 30. The switch 30 is
3 implemented by hardware, such as a layer 4 switch, or
4 software, for intercepting information exchanged across the
5 network without a sender and a recipient being aware of it.

6 In this example embodiment, while assuming the business
7 communication, the digital signature system is employed for
8 the exchange of messages by the companies A and B. However,
9 the digital signature system in this embodiment can be
10 applied not only for business communications, but also for
11 communications between specific groups and for the exchange
12 of e-mails by the groups or individuals.

13 The configuration in Figure 1, is merely an example, and
14 another configuration may be employed so long as the
15 applications 10 and the signature server 20 are provided as
16 a single group, many of which are connected via the network.
17 Therefore, the switches 30 and the firewalls 40 are not
18 always requisite components. It should be noted, however,
19 that the firewall 40 is provided in this embodiment while
20 taking inter-company communications into account. Further,
21 the signature server 20 is connected via the switch 30 in
22 order to intercept communications between the applications
23 10 without changing the applications 10, and to add and
24 manage digital signatures.

25 In addition, in this embodiment, it should be noted that XML
26 documents are exchanged through inter-company communications
27 between the companies A and B (or between the applications

1 10 of the companies A and B). However, this embodiment can
2 also be applied for documents other than XML documents, or
3 for e-mail.

4 In Figure 1, the application 10 prepares an XML message
5 document, such as a product order sheet, a product order
6 receipt sheet or a specification, that is required for
7 business, and transmits the XML document to the
8 corresponding application 10 of the other company.

9 The signature server 20 has a function for intercepting an
10 HTTP connection for message document transmission by the
11 local application 10 to the other company, and a function
12 (reverse proxy) for intercepting an HTTP connection from the
13 other company to a predetermined application 10 at the local
14 company. The signature server 20 provides a necessary
15 digital signature for the message document that is
16 intercepted during the transmission by the local company to
17 the other company, or verifies the digital signature
18 provided for the message document that is intercepted during
19 the transmission from the other company to the local
20 company. The detailed configuration and operation of for
21 the signature server 20 will be described later.

22 The switch 30 is provided between the applications 10 and
23 the firewall 40 located at the border (entrance/exit)
24 between the LAN 100 and the network 200, and connects the
25 signature server 20 and the LAN 100, so that the signature
26 server 20 can intercept the HTTP connections. It should be
27 noted that communication can also be effected via the
28 signature server 20 by changing the URLs of the applications

1 10, instead of using the switch 30. However, when the
2 switch 30 is used, the applications 10 need not be changed,
3 and the signature server 20 can add and manage a digital
4 signature.

5 High security is required for the platform (OS) of the
6 signature server for the following reasons:

- 7 1. A secret key used for a signature should not be
8 stolen.
- 9 2. The key for a root verification center for
10 verifying the signature should not be rewritten.
- 11 3. The access control afforded for a log should not be
12 bypassed.

13 Thus, common internet access to the signature server 20
14 should be inhibited, or very limited. Therefore, a method
15 can be employed for using a network address (e.g., a local
16 address, such as 192.168.xx.xx) so that the proxy can not be
17 externally accessed. There is also another method whereby
18 an intercepted packet is converted into a medium, such as an
19 RS-232C or USB, that generally does not pass through the
20 TCP/IP, and for later transmitting the packet to the
21 signature server 20. Using these methods provides better
22 security for the key and the log.

23 Figure 2 is a diagram showing an example configuration of
24 the signature server 20 for adding a digital signature. The
25 digital signature used in this embodiment is an XML digital
26 signature provided by public key cryptography using a hash
27 function.

1 In Figure 2, the signature server 20 includes: a signature
2 key determiner 21, for selecting a secret key used for
3 providing a digital signature; a key manager 22, for
4 managing the secret key; a signature key acquisition unit
5 23, for obtaining a necessary secret key from the key
6 manager 22 in accordance with the selection of the signature
7 key determiner 21; a signature generator 24, for generating
8 signature information using the secret key obtained by the
9 signature key acquisition unit 23, and for providing a
10 signature for a message document; and a log manager 25, for
11 managing the log for the message document.

12 The signature key determiner 21 obtains an XML message
13 document from the application 10 of the local company, and
14 selects, according to a predetermined key selection rule, a
15 secret key that is required to provide an appropriate
16 signature for the XML document. The key selection rule is a
17 rule for selecting the secret key based on the contents of
18 the XML document, and is written using the XML format, for
19 example.

20 For the digital signature added to the XML document, various
21 definitions can be set. For example: the date stamp
22 automatically added to all the documents to be transmitted
23 to the other companies; a signature provided by the person
24 in charge after the signature has been examined; the
25 official stamp of the company; or a signature having an
26 intermediate characteristic of these. The signature
27 definition is determined from the definition of the

1 signature key (normally written as a verification practice
2 statement in a digital certificate corresponding to the
3 signature key).

4 As is described above, different secret keys can be employed
5 in accordance with the contents of the XML document. This
6 can be implemented when the signature key determiner 21
7 registers as a rule a set of contents for the XML document
8 and a corresponding secret key. Since the contents of the
9 XML document are represented by using XPath, a complicated
10 pattern can be designated, and further, a specific range in
11 the XML document can be designated as a signing range.

12 Figure 6 is a diagram showing an example key selection rule
13 written using the XML format. In this example, it is
14 determined that for electronic commerce the company seal
15 will be employed as a secret key for a digital signature for
16 a transaction whereof the price is equal to or greater than
17 one million yen, and that the seal of the person in charge
18 will be employed as the secret key for a transaction whereof
19 the price is equal to or greater than 100,000 yen.

20 The key manager 22 manages the secret key used for providing
21 a digital signature for the XML document. The key manager
22 can also set the key acquisition condition (key selection
23 rule) for the secret key prepared for the digital signature,
24 and can manage this condition. Specifically when the
25 acquisition condition, such as the time for the use of the
26 secret key or the process to be performed in advance, is
27 established, the use of the corresponding secret key is

1 permitted, whereas in other cases, the use of the secret key
2 is inhibited. Permission for the use of the secret key can
3 be controlled, for example, by loading or unloading the data
4 for the secret key.

5 For example, when the time condition for permitting signing
6 only within a specific time period in a day is set for a
7 predetermined digital signature, the secret key required for
8 the generation of the pertinent digital signature is loaded
9 for the time period to permit the use of the key.

10 When the acquisition condition is set, such a condition is
11 established to obtain the secret key, so that the
12 reliability of the digital signature provided using the
13 secret key can be increased.

14 The signature key acquisition unit 23 obtains, from the key
15 manager 22, the secret key that is selected, in accordance
16 with the contents of the XML document, by the signature key
17 determiner 21, and transmits the secret key to the signature
18 generator 24. As is described above, when the acquisition
19 condition for the secret key has not been established at the
20 time whereat the signature key determiner 21 selects the
21 secret key, a default replacement secret key (hereinafter
22 referred to as a replacement key) can be transmitted to the
23 signature generator 24. In this case, when the acquisition
24 condition for the secret key selected by the signature key
25 determiner 21 is finally established, the original secret
26 key can be obtained and transmitted to the signature
27 generator 24.

1 When the time restriction is set as the acquisition
2 condition, and when the time where signature key acquisition
3 unit 23 attempts to obtain the secret key is not within time
4 period where the secret key is loaded into the key manager
5 22, the signature key acquisition unit 23 transmits the
6 replacement key to the signature generator 24. When the
7 time where the secret key is to be loaded into the key
8 manager 22 is reached, the signature key acquisition unit 23
9 obtains the secret key from the key manager 22, and
10 transmits it to the signature generator 24.

11 The signature generator 24 provides a digital signature for
12 the XML document using the secret key obtained by the
13 signature key acquisition unit 23. In principle, the target
14 XML document is the one transmitted by the application 10,
15 and intercepted by the switch 30. However, as is described
16 above, when the acquisition condition is set for the secret
17 key, and when a digital signature has been provided using
18 the replacement key for the XML document obtained by
19 intercepting, the original secret key is obtained and the
20 digital signature is again provided for the XML document by
21 using the secret key. In this case, the post digital
22 signature using the secret key may be added for the XML
23 document with the digital signature using the replacement
24 key, or may be newly provided for the XML document in the
25 state before the digital signature is provided using the
26 replacement key. The XML document accompanied by a digital
27 signature provided by the signature generator 24 is returned
28 to the LAN 100 and is transmitted to the destination
29 designated by the application 10, and is also transmitted to

1 the log manager 25 and managed therein.

2 The log manager 25 obtains and manages the log of the XML
3 document with the digital signature provided by the
4 signature generator 24. Generally, the XML document with
5 the digital signature is safely stored for future
6 monitoring. The log can be obtained by the application 10
7 or during communication; however, it is optimal for the log,
8 including an effective signature, to be obtained at the time
9 of signing or verification, because then it can be ensured
10 that the signature is authenticated when the log is
11 obtained. If the log is not obtained at the time of
12 signing, a problem arises in that an object, to which the
13 signature is provided, that can not be monitored may occur
14 later.

15 To obtain the log of the XML document with a signature, the
16 XML document signed by the signature generator 24 need only
17 be stored in a long-term stable storage device (e.g., a hard
18 disk). Since a digital signature accompanies the stored XML
19 document, the illegal alteration of the log can be
20 prevented.

21 Further, since the log may include highly confidential
22 information, such as a credit card number, appropriate
23 access limits should be set for the log access. Access
24 control can also be applied for only one part of the log
25 (e.g., only for the credit card number).

26 In addition, as is described above, when the condition is

1 set for obtaining the secret key, an XML document without a
2 digital signature can also be stored and managed, so that
3 the digital signature can be newly added later using the
4 secret key to an XML document that has already been signed
5 using the replacement key.

6 Figure 3 is a diagram showing the configuration of the
7 signature server 20 for verifying a digital signature. In
8 Figure 3, the signature server 20 includes: a signature
9 information acquisition unit 31, for obtaining the signature
10 information for a digital signature from a received message
11 document; a key manager 32, for managing a public key used
12 to verify the signature information; a verification unit 33,
13 for verifying the digital signature based on the obtained
14 signature information; and a log manager 34, for managing
15 the log of the received message document.

16 The signature information acquisition unit 31 externally
17 receives the XML message document. Then, the signature
18 information acquisition unit 31 obtains the signature
19 information for the digital signature added to the XML
20 document, and also, based on the information written in the
21 XML document, acquires from the key manager 32 the public
22 key required for verifying the XML document and transmits it
23 to the verification unit 33.

24 The key manager 32 manages the public key used to verify the
25 digital signature provided for the XML document. The public
26 key corresponding to the secret key used for signing the XML
27 document may be stored in storage means in the signature

1 server 20 or in a network system, or the public key may be
2 obtained from an external examination organization via a
3 network.

4 The verification unit 33 verifies the digital signature
5 using the public key that corresponds to the contents of the
6 XML document. When the XML document is authenticated, the
7 verification unit 33 returns the XML document via the LAN
8 100 to the destination application 10, and also transmits
9 the XML document to the log manager 34. When the
10 authentication of the XML document has not been verified,
11 the verification unit 33 performs a predetermined error
12 process, without returning the XML document to the LAN 100.
13 When a digital signature added to the XML document is one
14 provided not by using the secret key corresponding to the
15 contents of the XML document but by using a predetermined
16 replacement key (this can be confirmed by selecting the
17 public key to verify the digital signature), the
18 verification unit 33 determines the final authorization for
19 the digital signature upon the receipt of the XML document
20 that was signed by using the original secret key.

21 In this case, the XML document that was signed by using the
22 replacement key either may be held by the signature server
23 20 until the XML document signed by the original secret key
24 is received, or may be transmitted to the application 10
25 without waiting for the receipt of the XML document signed
26 by using the secret key, so that the process may be
27 advanced. In any case, the effective period of the XML
28 document signed using the replacement key is defined, and

1 when the XML document signed using the original secret key
2 does not arrive within the effective period, the XML
3 document signed using the replacement key is determined to
4 be invalid. It should be noted that means for comparing
5 document IDs can be employed to correlate the XML document
6 signed using the replacement key with the XML document
7 signed using the original secret key.

8 As an example of the effective performance of the digital
9 signature method using the replacement key, a process may be
10 initiated for an XML document signed using a replacement
11 key, and when an XML document signed using an original
12 secret key does not arrive within a predetermined period of
13 time, the process that is currently being performed may be
14 invalidated.

15 The log manager 34 obtains and manages the XML document
16 using a signature verified by the verification unit 33 and
17 the log of the verification results.
18 To obtain the log of the signed XML document, the XML
19 document verified by the verification unit 33 need only be
20 stored on a long-term stable storage device (a hard disk).
21 Since the stored XML document is accompanied by a digital
22 signature, the illegal alteration of the log can be
23 prevented. When the stored log data is compared with the
24 log data stored by the log manager 25 of the signing
25 execution side in the signature server 20 of the transaction
26 partner, the completeness of the log data is ensured and the
27 operational security can be improved.

1 The comparison of the log data need not be performed for all
2 the signed XML documents in the log of the log manager 25,
3 and the signature information for the digital signature,
4 especially the hash value used for the signature, need only
5 be compared. As an example, assume the comparison of the
6 log data for a message transmitted between the companies A
7 and B in Figure 1. In this example, the hash values in the
8 log data of the companies A and B are exchanged and compared
9 for each predetermined time, such as monthly. When the hash
10 values used for the message communication between the
11 companies A and B match, it is ascertained that all the
12 messages have been verified by both companies A and B using
13 the digital signature. When the hash values differ, it is
14 ascertained that there is a message that has not been
15 verified by either company A or B. Then, all the log data
16 are exchanged to search for the message document that has
17 not been verified by the company A or B.

18 The individual components of the signature server 20 in
19 Figs. 2 and 3 are virtual software blocks implemented by a
20 CPU that is controlled by a computer program. The computer
21 program for controlling the CPU is provided by being stored
22 on storage medium such as a CD-ROM or a floppy disk, or by
23 being transmitted via a network.

24 Furthermore, in the above explanation, the digital signature
25 addition configuration and the digital signature
26 verification configuration are separately shown for the same
27 signature server 20; however, the proxy server in Figure 2
28 and the proxy server in Figure 3 may be separately provided.

1 An explanation will now be given for the post signing
2 processing performed by the key manager 22, the signature
3 key acquisition unit 23, the signature generator 24 and the
4 log manager 25 of the signature server 20 in Figure 2.
5 Figure 4 is a flowchart for explaining the signing
6 processing, including a case wherein the original secret key
7 can not be employed.

8 In Figure 4, first, the signature key acquisition unit 23
9 inquires of the key manager 22 whether the secret key
10 selected by the signature key determiner 21 can be used
11 (step 401). If the secret key can be used, it is obtained
12 and transmitted to the signature generator 24. The
13 signature generator 24 uses the secret key to provide a
14 digital signature for an XML document, and transmits the
15 obtained XML document (step 402). The processing is
16 thereafter terminated.

17 If the secret key can not be used because its acquisition
18 condition has not been established, the signature key
19 acquisition unit 23 obtains a default replacement key from
20 the key manager 22, and transmits the replacement key to the
21 signature generator 24. The signature generator 24 provides
22 a digital signature for an XML document using the
23 replacement key, and transmits the obtained XML document
24 (step 403). The log manager 25 writes the XML document into
25 a post signing log that has been prepared (step 404). When
26 the secret key is used later to additionally provide a
27 digital signature for the XML document that was signed using
28 the replacement key, the XML document signed using the

1 replacement key is stored in the post signing log. When the
2 secret key is used later to newly provide a digital
3 signature for the XML document that has not yet been signed
4 using the replacement key, the XML document without the
5 signature is stored in the post signing log.

6 Figure 5 is an example of a flowchart for explaining the
7 processing performed when the acquisition condition for a
8 predetermined secret key is established and the secret key
9 is available. In Figure 5, when the predetermined secret
10 key is available, the log manager 25 determines whether
11 there is an XML document for which the post signing using
12 the secret key is required (steps 501 and 502). If there is
13 such an XML document in the post signing log, the signature
14 generator 24 receives the secret key from the signature key
15 acquisition unit 23 and the XML document from the log
16 manager 25, provides a digital signature for the XML
17 document using the secret key, and transmits the obtained
18 XML document (steps 503 and 504).

19 As is described above, when a required secret key can not be
20 used, a digital signature is provided for a document using a
21 replacement key, and the document is transmitted (Figure 4),
22 and when the secret key can be used, a digital signature is
23 provided for the document later and the obtained document is
24 transmitted (Figure 5).

25 It is assumed that unique serial numbers are provided for
26 digital signatures. Thus, when a post signature has been
27 provided, or when the same message has been transmitted

1 twice due to an erroneous process, the operation based on
2 the message document (e.g., an order reception process in
3 response to the order using the message document) can
4 prevent overlapping.

5 Thus, as is described above according to the invention,
6 since the means for providing, verifying or logging a
7 digital signature for a message exchanged over a network is
8 mounted as a proxy server, the security function using the
9 digital signature can be improved without a change of an
10 application program being required.

11 Further, according to the invention, a post signing method
12 can be provided by controlling the digital signature and its
13 verification using a proxy server. In addition, according
14 to the invention, enable access control can be exercised for
15 the log of a message by logging a message using a proxy
16 server.

17 The present invention can be realized in hardware, software,
18 or a combination of hardware and software. A visualization
19 tool according to the present invention can be realized in a
20 centralized fashion in one computer system, or in a
21 distributed fashion where different elements are spread
22 across several interconnected computer systems. Any kind of
23 computer system - or other apparatus adapted for carrying out
24 the methods and/or functions described herein - is suitable.
25 A typical combination of hardware and software could be a
26 general purpose computer system with a computer program that,
27 when being loaded and executed, controls the computer system

1 such that it carries out the methods described herein. The
2 present invention can also be embedded in a computer program
3 product, which comprises all the features enabling the
4 implementation of the methods described herein, and which -
5 when loaded in a computer system - is able to carry out these
6 methods.

7 Computer program means or computer program in the present
8 context include any expression, in any language, code or
9 notation, of a set of instructions intended to cause a system
10 having an information processing capability to perform a
11 particular function either directly or after either
12 conversion to another language, code or notation, and/or
13 reproduction in a different material form.

14 Thus the invention includes an article of manufacture which
15 comprises a computer usable medium having computer readable
16 program code means embodied therein for causing a function
17 described above. The computer readable program code means
18 in the article of manufacture comprises computer readable
19 program code means for causing a computer to effect the
20 steps of a method of this invention. Similarly, the present
21 invention may be implemented as a computer program product
22 comprising a computer usable medium having computer readable
23 program code means embodied therein for causing a function
24 described above. The computer readable program code means
25 in the computer program product comprising computer readable
26 program code means for causing a computer to effect one or
27 more functions of this invention. Furthermore, the present
28 invention may be implemented as a program storage device

1 readable by machine, tangibly embodying a program of
2 instructions executable by the machine to perform method
3 steps for causing one or more functions of this invention.

4 It is noted that the foregoing has outlined some of the more
5 pertinent objects and embodiments of the present invention.
6 This invention may be used for many applications. Thus,
7 although the description is made for particular arrangements
8 and methods, the intent and concept of the invention is
9 suitable and applicable to other arrangements and
10 applications. It will be clear to those skilled in the art
11 that modifications to the disclosed embodiments can be
12 effected without departing from the spirit and scope of the
13 invention. The described embodiments ought to be construed
14 to be merely illustrative of some of the more prominent
15 features and applications of the invention. Other beneficial
16 results can be realized by applying the disclosed invention
17 in a different manner or modifying the invention in ways
18 known to those familiar with the art.